ABSTRACT

[0070] A user terminal can be authenticated by an access point based on one message. In one embodiment, the present invention includes the access point receiving a message containing a shared secret encrypted with an access point public key, a user terminal certificate, and an authenticator string demonstrating possession by the user terminal of a user terminal private key. The access point can decrypt the shared secret using the private key of the access point paired with its private key. The access point can then authenticate the user terminal by checking the authenticator string using a user terminal public key included in the user terminal certificate to verify possession of the user terminal private key by the user terminal.